
		Chicago Police Department		General Order G0			
ELECTRONIC SIGNATURES							
							
ISSUE DATE:		22 February 2012		EFFECTIVE DATE:		22 February 2012	
RESCINDS:		Version dated 13 February 2007; G98-07-08					
INDEX CATEGORY:		Information Management					

I. PURPOSE

This directive:

- A. specifies the responsibilities of Department members who utilize electronic signatures for authentication and approval of Department reports and forms generated by automated applications.
- B. continues the use of the Sworn Electronic Signature Verification Affidavit (CPD-62.111).
- C. introduces the Civilian Electronic Signature Verification Affidavit (CPD-62.112).

II. GENERAL INFORMATION

- ~~A.~~ Department members will use their logon username (PC Number) and password to access Department automated applications.
- ~~B.~~ For reports generated by a Department automated application, the signature and affirmation requirements listed in the Department directive entitled "Department Reports and Letters of Clearance" will be satisfied by the member's electronic signature. **A Department member entering his or her logon username and password into the application will act as his or her electronic signature and will have the full effect as that of the member's written signature. Department members will be responsible for any access to the Department's automated applications by their username and password.**
- C. **All Department members outlined in Item III-A of this directive are required to sign a signature verification affidavit appropriate to their status. Department members who have previously completed a signature verification affidavit, prior to the issue date of this directive, have not satisfied the signature requirement of this directive.**


III. APPLICATION ACCESS

- A. The following personnel, identified by their logon username, will have access to the Department's computer databases and automated applications and have the ability to electronically sign automated Department reports and forms:
 - 1. All Department members of exempt rank, sworn or civilian.
 - 2. All sworn Department members.

CL# 1050637
Attachment # 28
1 of 3

3. Select civilian Department members identified and designated by their unit commanding officer to utilize automated applications and authorized by the appropriate exempt Department member.
- B. Department members will be assigned a role, based on rank and assigned duty, which determines the level of access provided as users of the automated application.
- C. If a unit commanding officer has occasion to request a permanent change in the role of a member, the unit commanding officer will submit a To-From-Subject report through the chain of command to the Managing Deputy Director, Public Safety Information Technology, and include the member's name, logon username, and level of access to be granted to the automated application.

IV. RESPONSIBILITIES

- A. Department members, as outlined in Item III-A of this directive, will:
 1. complete and sign the appropriate Electronic Signature Verification Affidavit and submit the affidavit to their station supervisor/unit commanding officer.
 - a. Sworn Department members will complete the Sworn Electronic Signature Verification Affidavit.
 - b. Civilian Department members will complete the Civilian Electronic Signature Verification Affidavit.
 -  2. take precautions to maintain strict confidentiality of the password associated with their logon username.
- B. Station supervisors/unit commanding officers will ensure:
 1. each Department member under their command, as outlined in Item III-A of this directive, completes the appropriate Electronic Signature Verification Affidavit.
 2. submitted Electronic Signature Verification Affidavit forms are complete, including the witness section verifying the affidavit.
 3. completed Electronic Signature Verification Affidavit forms are forwarded to the Human Resources Division without delay.
- C. Unit commanding officers will ensure Department members under their command are assigned the appropriate role and level of access to the Department's automated applications. If a unit commanding officer has occasion to request a change in the role of a member, the unit commanding officer will follow the procedures outlined in Item III-C of this directive.
- D. The Director, Human Resources Division, will:

CL# 1050637
Attachment# 28
Page 2 of 3

1. ensure new Department employees, on their date of hire, complete the appropriate Electronic Signature Verification Affidavit.
2. retain all completed Electronic Signature Verification Affidavit forms in each member's personnel jacket in accordance with existing records retention requirements.

E. The Managing Deputy Director, Public Safety Information Technology, will:

1. ensure members are granted security access to the Department's computer databases and automated application systems as deemed necessary by their unit commanding officer.
2. provide the necessary training and support to ensure that units are capable of fulfilling the requirements of this directive.

V. **PASSWORDS**

If Department members forget their password or the password has been compromised, members will:

- A. immediately notify their supervisor,
- B. contact the Help Desk, and
- C. follow the procedures provided by Help Desk personnel to complete the password change process.

(Items indicated by italic/double underline were added or revised)

Garry F. McCarthy
Superintendent of Police

06-082/12-003 MAV/MWK(PMD)/TRH

CL# 1050637
Attachments 28
Page 3 of 3